(12) (9)文献

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-328460
(43)Date of publication of application : 30.11.1999

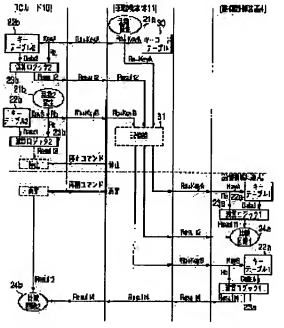
(51)Int.Cl. G07B 15/00

(21)Application number : 10-125923
(22)Date of filing : 08.05.1998

(71)Applicant : MITSUBISHI HEAVY IND LTD
(72)Inventor : YASUI MASAYUKI

(54) METHOD FOR MUTUALLY CERTIFYING IC CARD FOR PAY ROAD

(57)Abstract:
PROBLEM TO BE SOLVED: To surely operate mutual certification of an IC card within a prescribed time in an inexpensive system, and to maintain security.
SOLUTION: When an IC card 10 is inserted, an on-vehicle equipment main body 11 transmits a random number 1 (Ra) and a key code (Key A) to the IC card 10 so that a certification operation can be executed. In the on-vehicle equipment main body 11, the random number 1 (Ra), key code (Key A), the arithmetic result 2 (result 2) of the IC card 10, random number 2 (Rb), and key code (Key B) are stored in a storage part 31, and a stop command is transmitted to the IC card 10. When the on-vehicles device enters a communication area in this state, the on-vehicle equipment main body 11 transmits the storage information in the storing part 31 to a road side controller 4 so that the certification operation can be executed, and transmits a resume commands and an arithmetic result 4 (Result 4) of the road side controller 4 to the IC card 10. The IC card 10 confirms the validity of the road side controller 4 according to the already obtained arithmetic result 3 (Result 3) and the arithmetic result 4 (Result 4).



LEGAL STATUS

[Date of request for examination]	17.04.2003
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3697061
[Date of registration]	08.07.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平11－328460

(43)公開日　平成11年(1999)11月30日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｇ０７Ｂ　15/00	５１０	Ｇ０７Ｂ　15/00	５１０

審査請求　未請求　請求項の数２　ＯＬ　（全７頁）

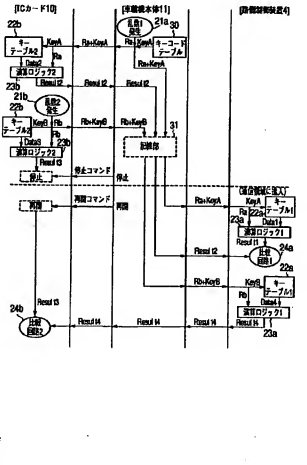
(21)出願番号　特願平10－125923

(22)出願日　平成10年(1998)５月８日

(71)出願人　000006208
三菱重工業株式会社
東京都千代田区丸の内二丁目５番１号
(72)発明者　泰井　真之
兵庫県神戸市兵庫区和田崎町一丁目１番１号　三菱重工業株式会社神戸造船所内
(74)代理人　弁理士　鈴江　武彦　（外５名）

(54)【発明の名称】　有料道路のＩＣカード相互認証方法

(57)【要約】
【課題】安価なシステムで所定の時間内でＩＣカードの相互認証を確実に行ない、且つ、高いセキュリティを保持する。
【解決手段】車載機本体１１はＩＣカード１０が挿入されると、乱数１（Ra）とキーコード（Key Ａ）をＩＣカード１０へ送信し認証演算を実行させる。車載機本体１１は、乱数１（Ra）、キーコード（Key Ａ）、ＩＣカード１０の演算結果２（Result２）、乱数２（Rb）、キーコード（Key Ｂ）を記憶部３１に記憶し、ＩＣカード１０に停止コマンドを送信する。この状態で車載装置が通信領域に進入すると、車載機本体１１は記憶部３１の記憶情報を路側制御装置４へ送信し認証演算を実行させると共に、ＩＣカード１０に再開コマンド及び路側制御装置４の演算結果４（Result４）を送信する。ＩＣカード１０は、既に求めた演算結果３（Result３）と演算結果４（Result４）により路側制御装置４の正当性を確認する。



【特許請求の範囲】

【請求項１】　料金収受用のＩＣカード及び無線通信機能を備えた車載機本体からなる車載装置を車両に搭載し、有料道路の料金所に設置される路側制御装置との間で無線通信により情報を交換して料金収受を行なう際に、相手方の正当性を相互に認証する有料道路のＩＣカード相互認証方法において、

前記車載機本体に乱数発生部、キーコードテーブルを設けると共に、認証情報記憶用の記憶部を設け、前記車載機本体はＩＣカードが挿入されると、前記乱数発生部により乱数を発生させると共にキーコードテーブルよりキーコードを選択してＩＣカードへ送信して認証演算を実行させ、前記乱数、キーコード、及び前記ＩＣカードの演算結果を前記記憶部に記憶した後、前記ＩＣカードに停止コマンドを送信して該ＩＣカードの相互認証動作を一時停止させ、

前記車両に搭載された車載装置が料金所の通信領域に進入すると、車載機本体は前記記憶部の記憶情報を路側制御装置へ送信して認証演算を実行させると共に、前記ＩＣカードに再開コマンド及び前記路側制御装置の認証結果を送信して該路側制御装置に対する認証動作を実行させることを特徴とする有料道路のＩＣカード相互認証方法。

【請求項２】前記記憶部は、認証完了後またはＩＣカードが車載機本体から引き抜かれた場合に記憶内容がクリアされるように構成したことを特徴とする請求項１記載の有料道路のＩＣカード相互認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、有料道路の通行料金自動徴収システムにおけるＩＣカードの相互認証方法に関する。

【０００２】

【従来の技術】図２は、本発明の対象とする有料道路の通行料金自動徴収システムの機器構成例を示すものである。図２において、１は車両、２は車両１に搭載される車載装置、３は料金所キャノピーなど路側に固定設置される路側アンテナ、４は車載装置２と路側アンテナ３間の通信制御及びデータ処理を行なう路側制御装置、５は路側アンテナ３と車載装置２との間で通信が可能な通信領域５を示す。

【０００３】車載装置２を搭載した車両１が料金所に近づき、通信領域５に進入すると、車載装置２と路側アンテナ３との間で無線通信が行なわれ、料金収受に必要な情報例えば経路情報、金額情報等が交換され、通行料金が自動的に徴収される。

【０００４】図３は、本発明の対象とする車載装置２の構成例を示すものである。車載装置２は、大別してＩＣカード１０と車載機本体１１に分けられる。ＩＣカード１０は、マイクロプロセッサ及びメモリを内蔵したコンタクト型カードで、金額情報、個人情報など高いセキュリティを必要とするデータが格納されている。

【０００５】車載機本体１１は、ＩＣカード１０とのデータ転送するためのＩＣカードコンタクト部１２及びＩＣカードインターフェイス回路１３、上記路側アンテナ３と無線通信するためのアンテナ１５及び無線制御部１６、車両１内の運転者とインターフェイスとなる表示部１７及び入力部１８、これらＩＣカード１０、無線通信、表示、入力及びデータを処理、記憶するマイクロプロセッサ１４から構成される。

【０００６】そして、車載装置２を使用する時は、ＩＣカード１０を車載機本体１１に挿入した状態で有料道路を走行し、料金所の通信領域５に進入することで、ＩＣカード１０内の残額情報、個人情報が車載機本体１１を経由して路側アンテナ３及び路側制御装置４へ送信される。路側制御装置４で受信したＩＣカード１０の残額情報、個人情報に基づきデータチェックを行ない、問題がなければ通行料金の引き去り後、新しい金額情報を路側アンテナ３、車載機本体１１を経由してＩＣカード１０へ書込む。

【０００７】上記のようにして通行車両１に対する料金収受処理が行なわれるが、ＩＣカード１０内の金額情報、個人情報は、不正防止、秘匿性の観点より高いセキュリティが要求される。一般的に使用される不正防止方法としては、各々相手方の正当性を確認する相互認証方法が用いられている。

【０００８】図４は、一般的なＩＣカードの認証方法例を示したものである。ＩＣカード１０及びＩＣカード端末機は、それぞれ乱数発生部２１ａ、２１ｂ、キーコードに対応する認証用データを格納するキーテーブル２２ａ、２２ｂ、認証用演算ロジック２３ａ、２３ｂ、演算結果を比較する比較回路２４ａ、２４ｂを有する。

【０００９】まず、ＩＣカード端末機からＩＣカード１０を認証する場合について説明する。ＩＣカード端末機側の乱数発生部２１ａで乱数１（Ｒａ）を発生させ、キーテーブル２２ａよりキーコード（Ｋｅｙ Ａ）を任意に選定する。ＩＣカード端末機は乱数１（Ｒａ）とキーコード（Ｋｅｙ Ａ）に対応する認証用データ（Ｄａｔａ１）より演算ロジック２３ａにて認証演算を行ない、演算結果１（Ｒｅｓｕｌｔ１）を得る。

【００１０】一方、乱数１（Ｒａ）とキーコード（Ｋｅｙ Ａ）はＩＣカード１０へ送信され、ＩＣカード１０は乱数１（Ｒａ）とキーテーブル２２ｂよりキーコード（Ｋｅｙ Ａ）に対応する認証用データ（Ｄａｔａ２）を取出し、演算ロジック２３ｂにて認証演算を行ない、演算結果２（Ｒｅｓｕｌｔ２）を得る。ＩＣカード１０の演算結果２（Ｒｅｓｕｌｔ２）は、ＩＣカード端末機に送信され、ＩＣカード端末機の比較回路２４ａにてＩＣカード端末機の演算結果１（Ｒｅｓｕｌｔ１）とＩＣカード１０の演算結果２（Ｒｅｓｕｌｔ２）が比較され、結果が一致していればＩＣカード１０

の正当性を確認できる。

【００１１】次に、ＩＣカード１０からＩＣカード端末機を認証する場合について説明する。ＩＣカード１０からＩＣカード端末機を認証する場合には、ＩＣカード１０側で乱数発生部２１ｂから乱数２（Ｒｂ）を発生させ、キーテーブル２２ｂよりキーコード（Ｋｅｙ Ｂ）を任意に選定し、乱数２（Ｒｂ）と認証用データ（Ｄａｔａ３）より演算ロジック２３ｂにて認証演算を行ない、演算結果３（Ｒｅｓｕｌｔ３）を得る。

【００１２】上記乱数２（Ｒｂ）とキーコード（Ｋｅｙ Ｂ）は、ＩＣカード端末機に送信され、ＩＣカード端末機は乱数２（Ｒｂ）とキーテーブル２２ａよりキーコード（Ｋｅｙ Ｂ）に対応する認証用データ（Ｄａｔａ４）を取出し、演算ロジック２３ａにて認証演算を行ない、演算結果４（Ｒｅｓｕｌｔ４）を得る。この演算結果４（Ｒｅｓｕｌｔ４）は、ＩＤカードへ送信され、ＩＣカード１０の比較回路２４ｂにてＩＣカード演算結果３（Ｒｅｓｕｌｔ３）とＩＣカード端末機の演算結果４（Ｒｅｓｌｔ４）が比較され、結果が一致していればＩＣカード１０はＩＣカード端末機の正当性を確認できる。

【００１３】

【発明が解決しようとする課題】図４の例では、ＩＣカード１０とＩＣカード端末機が持つキーテーブル２２ａ及び演算ロジック２３ａが解読されると不正使用される恐れがあり、このキーテーブル２２ａ及び演算ロジック２３ａの高いセキュリティ性が必要となる。

【００１４】一般的にＩＣカード１０のキーテーブル２２ｂ、演算ロジック２３ｂは、ＩＣチップ内に格納されており、高いセキュリティを有する。一方、ＩＣカード端末機は、通常、銀行やデパート等の店舗に固定設置され、一般の利用者が安易に手を触れない場所にあり、店舗自体のセキュリティを上げることでＩＣカード端末機のキーテーブル２２ａ、演算ロジック２３ａのセキュリティが守られている。

【００１５】しかし、有料道路の通行料金自動徴収システムの場合、図３に示した車載機本体１１がＩＣカード端末機となる。車載機本体１１は、不特定多数の一般利用者に配られるため、悪意を持つ利用者が車載機本体１１を分解し、車載機本体１１内の認証用キーテーブル、演算ロジックを解析する可能性がある。

【００１６】また、車載機本体１１を単なる中継機とし、ＩＣカード１０と図２に示した路側制御装置４間で相互認証を行なう方法が考えられるが、車載装置２と路側アンテナ３間が通信可能な時間は通信領域５の大きさと車両走行速度に影響される。例えば通信領域５を３ｍ、車両走行速度を時速５４ｋｍと仮定すると、車載装置２と路上アンテナ３間の通信時間は、「３ｍ÷５４ｋｍ／ｈ＝０．２秒」となり、この０．２秒以内に相互認証を完了させる必要がある。但し、通信領域５が小さい場合や車両走行速度が速くなると、通信可能な時間は更に短くなり、相互認証演算時間もそれに伴って短くする必要がある。更に、演算ロジックについてもセキュリティ性を高めるため複雑な演算式が必要であり、複雑な演算式ほど演算時間がかかる。

【００１７】一般的にＩＣカードのマイクロプロセッサは動作速度が遅く、複雑な演算式を計算するのに数百ｍｓの時間が必要であり、走行中の車両に搭載されたＩＣカードと路側制御装置間で相互認証することは時間的に困難である。

【００１８】その対策として、ＩＣカードの演算時間を早くするためマイクロプロセッサの動作速度を早くする方法や数値演算プロセッサを搭載する方法が考えられるが、これらの方法ではＩＣカードが高価なものになるという問題があった。

【００１９】本発明は上記の課題を解決するためになされたもので、車載機本体に高いセキュリティが必要なキーテーブルと演算ロジックを格納する必要がなく、ＩＣカードに使用されるマイクロプロセッサの動作速度が遅くても料金収受処理を円滑に行なうことができる有料道路のＩＣカード相互認証方法を提供することを目的とする。

【００２０】

【課題を解決するための手段】第１の発明は、料金収受用のＩＣカード及び無線通信機能を備えた車載機本体からなる車載装置を車両に搭載し、有料道路の料金所に設置される路側制御装置との間で無線通信により情報を交換して料金収受を行なう際に、相手方の正当性を相互に認証する有料道路のＩＣカード相互認証方法において、前記車載機本体に乱数発生部、キーコードテーブルを設けると共に、認証情報記憶部を設け、前記車載機本体はＩＣカードが挿入されると、前記乱数発生部により乱数を発生させると共にキーコードテーブルよりキーコードを選択してＩＣカードへ送信して認証演算を実行させ、前記乱数、キーコード、及び前記ＩＣカードの演算結果を前記記憶部に記憶した後、前記ＩＣカードに停止コマンドを送信して該ＩＣカードの相互認証動作を一時停止させ、前記車両に搭載された車載装置が料金所の通信領域に進入すると、車載機本体は前記記憶部の記憶情報を路側制御装置へ送信して認証演算を実行させると共に、前記ＩＣカードに再開コマンド及び前記路側制御装置の認証結果を送信して該路側制御装置に対する認証動作を実行させることを特徴とする。

【００２１】第２の発明は、前記第１の発明において、認証完了後またはＩＣカードが車載機本体から引き抜かれた場合に記憶部の記憶内容がクリアされるように構成したことを特徴とする。

【００２２】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態を説明する。図１は、本発明に係る有料道路のＩＣカード相互認証方法を説明するための図である。本

実施形態は、図２に示した路側制御装置４に、キーコードに対応する認証用データを格納するキーテーブル２２ａ、認証用演算ロジック２３ａ、この演算ロジック２３ａによる演算結果１（Result1）と車載機本体１１の演算結果を比較する比較回路２４ａを備えている。

【００２３】また、図３に示した車載機本体１１には、乱数発生部２１ａ、キーコードだけが格納されているキーコードテーブル３０、及び認証用の各データを記憶する記憶部３１を設けている。この記憶部３１は、認証完了後、またはＩＣカード１０が車載機本体１１から引き抜かれた場合に記憶内容がクリアされるようになっている。

【００２４】そして、図３に示したＩＣカード１０には、乱数発生部２１ｂ、キーテーブル２２ｂ、演算ロジック２３ｂ、比較回路２４ｂを設けている。次に本発明の実施形態に係る有料道路のＩＣカード相互認証方法について説明する。

【００２５】車両の走行に際し、ＩＣカード１０を車載機本体１１に挿入すると、車載機本体１１は乱数発生部２１ａより乱数１（Ra）を発生させ、キーコードだけが格納されているキーコードテーブル３０よりキーコード（Key A）を選択し、乱数１（Ra）とキーコード（Key A）をＩＣカード１０へ送信する。

【００２６】ＩＣカード１０は、乱数１（Ra）とキーテーブル２２ｂよりキーコード（KeyA）に対する認証用データ（Data2）を取出し、演算ロジック２３ｂにて認証演算を行ない、演算結果２（Result2）を得る。このＩＣカード１０の演算結果２（Result2）は、車載機本体１１へ送信される。

【００２７】次にＩＣカード１０は、乱数発生部２１ｂから乱数２（Rb）を発生させ、キーテーブル２２ｂよりキーコード（Key B）を任意に選定し、乱数２（Rb）とキーテーブル２２ｂから取り出した認証用データ（Data3）より演算ロジック２３ｂにて認証演算を行ない、演算結果３（Result3）を得る。上記乱数２（Rb）とキーコード（Key B）は、車載機本体１１へ送信される。

【００２８】車載機本体１１は、乱数発生部２１ａで発生した乱数１（Ra）、キーコード（Key A）、ＩＣカード１０から送信されてきた演算結果２（Result2）、乱数２（Rb）、キーコード（Key B）を一旦記憶部３１に記憶するとと共に、ＩＣカード１０に対して相互認証の一時停止を指示する停止コマンドをＩＣカード１０へ送信する。停止コマンドを受信したＩＣカード１０は、相互認証を一時停止する。

【００２９】この状態で図２に示すように車載装置２を搭載した車両１が通信領域５に進入し、車載装置２と路側アンテナ３の通信が可能となった場合、車載機本体１１は、まず記憶部３１に記憶していた車載機本体１１で発生した乱数１（Ra）とキーコード（Key A）を路側制御装置４へ送信し、続いてＩＣカード１０での演算結果２（Result2）を路側制御装置４へ送信する。

【００３０】路側制御装置４は、乱数１（Ra）とキーテーブル２２ａよりキーコード（KeyA）に対応する認証用データ（Data1）を取出し、演算ロジック２３ａにて認証演算を行ない、演算結果１（Result1）を得る。この演算結果１（Result1）と車載機本体１１の記憶部３１から送られてきたＩＣカード１０の演算結果２（Result2）とを比較回路２４ａで比較し、結果が一致していれば路側制御装置４はＩＣカード１０の正当性を確認できる。

【００３１】次に車載機本体１１は、記憶部３１に記憶している情報、すなわち、ＩＣカード１０より受信した乱数２（Rb）とキーコード（Key B）を路側制御装置４へ送信する。

【００３２】路側制御装置４は、乱数２（Rb）とキーテーブル２２ａよりキーコード（KeyB）に対応する認証用データ（Data4）を取出し、演算ロジック２３ａにて認証演算を行ない、演算結果４（Result4）を得る。この演算結果４（Result4）は、車載機本体１１に送信される。

【００３３】車載機本体１１は、通信領域５に進入することで、ＩＣカード１０に対して相互認証停止を解除するための再開コマンドを送信する。また、車載機本体１１は、路側制御装置４から受信した演算結果４（Result４）をＩＣカード１０へ送信する。

【００３４】ＩＣカード１０は、上記車載機本体１１からの再開コマンドにより動作を再開し、既に演算ロジック２３ｂで求めた演算結果３（Result3）と路側制御装置４の演算結果４（Result4）を比較回路２４ｂで比較し、路側制御装置４の正当性を確認する。この場合、ＩＣカード１０は、上記比較回路２４ｂでの比較結果が一致していれば、路側制御装置４の正当性を確認できる。

【００３５】車載機本体１１の記憶部３１は、上記認証完了後、またはＩＣカード１０が車載機本体１１から引き抜かれた場合に記憶内容がクリアされる。上記のように認証完了後、またはＩＣカード１０が車載機本体１１から引き抜かれた場合に記憶部３１の記憶内容をクリアすることにより、車載機本体１１を分解したとしても記憶部３１の記憶内容を盗み出すことは困難である。もし、記憶部３１の内容を読み出すことができたとしても、記憶部３１には乱数、キーコード、演算結果しか格納されていないので、それから認証用データ、認証ロジックを導き出すことは難しく、非常に高いセキュリティを持たせることができる。

【００３６】

【発明の効果】以上詳記したように本発明によれば、車載機本体にＩＣカードの認証演算を事前に実施するための必要最小限な乱数発生部、キーコードテーブルを設けると共に、乱数、キーコード、演算結果を記憶する記憶部を搭載し、ＩＣカード側の認証演算を料金所の通信領

域進入前に実施するようにしたので、車載機本体に高いセキュリティが必要なキーテーブルと演算ロジックを格納する必要がなく、安価に構成することができる。また、上記のようにＩＣカード側の認証演算を料金所の通信領域進入前に実施することにより、ＩＣカードに使用されるマイクロプロセッサの動作速度が遅くても、全くその影響を受けない。更に、車載機本体に設けた記憶部は、認証完了後、またはＩＣカードが引き抜かれた場合にクリアされるようにしているので、車載機本体を分解して記憶部の内容を盗み出すことは困難であり、もし、記憶部の内容を読み出すことができたとしても、記憶部には乱数、キーコード、演算結果しか格納されていないので、それらの情報から認証用データ、認証ロジックを導き出すことは難しく、非常に高いセキュリティを持たせることができる。従って、本発明による有料道路のＩＣカード相互認証方法を採用することにより、安価で不正防止に優れた有料道路の通行料金自動徴収システムを構築することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る有料道路のＩＣカード相互認証方法を示す図。

【図２】本発明の対象とする有料道路の通行料金自動徴収システムの機器構成例を示す図。

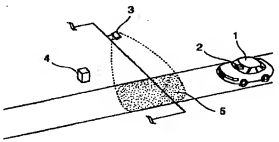
【図３】図２における車載装置の構成例を示すブロック＊図。

【図４】従来の有料道路のＩＣカード相互認証方法を示す図。

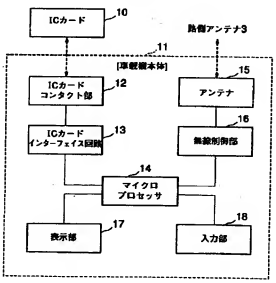
【符号の説明】

１　車両
２　車載装置
３　路側アンテナ
４　路側制御装置
５　通信領域
１１　車載機本体
１２　ＩＣカードコンタクト部
１３　ＩＣカードインターフェイス回路
１４　マイクロプロセッサ
１５　アンテナ
１６　無線制御部
１７　表示部
１８　入力部
２１ａ、２１ｂ　乱数発生部
２２ａ、２２ｂ　キーテーブル
２３ａ、２３ｂ　演算ロジック
２４ａ、２４ｂ　比較回路
３０　キーコードテーブル
３１　記憶部

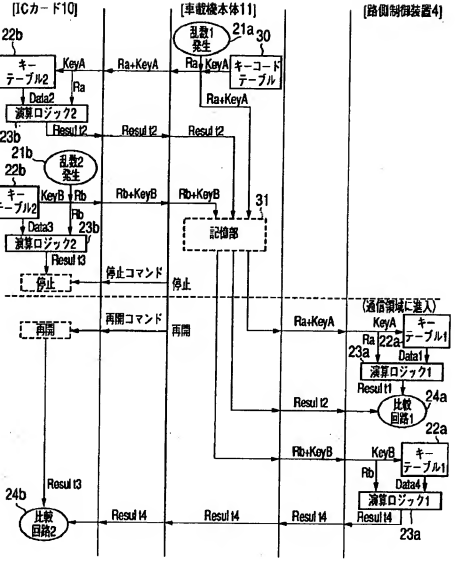
【図２】



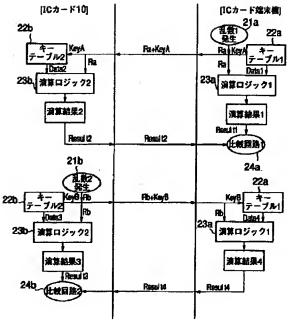
【図３】



【図１】


[ICカード10]
[車載機本体11]
[路側制御装置4]
乱数1発生
21a
30
22b
キーテーブル2
KeyA
Ra
Ra+KeyA
キーコードテーブル
Data2
演算ロジック2
Resul t2
23b
21b
乱数2発生
KeyB
Rb
Rb+KeyB
31
記憶部
Data3
Resul t3
停止
停止コマンド
(通信領域に進入)
再開
再開コマンド
キーテーブル1
22a
23a
Data1
演算ロジック1
Resul t1
比較回路1
24a
Data4
比較回路2
24b
Resul t4

【図４】


[ICカード10]
[ICカード端末機]
乱数1 発生
乱数2 発生
キーテーブル2
キーテーブル1
演算ロジック2
演算ロジック1
演算結果1
演算結果2
演算結果3
演算結果4
比較回路1
比較回路2
KeyA
KeyB
Ra
Rb
Data2
Data1
Data3
Data4
Ra+KeyA
Rb+KeyB
Result1
Result2
Result3
Result4
21a
21b
22a
22b
23a
23b
24a
24b